Remarks/Arguments

Claims 1-7 are pending. Claims 1 and 5 have been amended to more clearly and distinctly claim the subject matter that applicants regard as their invention. No new matter is believed to be added by the present amendment.

At the outset, applicants note that the examiner has provided somewhat differing statements regarding the basis for the rejection in view of Chaney and Santis. In the previous Office Action dated January 16, 2004, the examiner stated "... **Chaney ... does not explicitly express** using a first seed value received in said smart card and a second seed value, **said second seed value being permanently stored in said smart card**... (emphasis added)"

However, in the Response to Arguments section, the examiner states "the examiner agrees with the applicant that Chaney does not disclose the key based on the first seed value received in the smart card. However, **Chaney discloses a key that is permanently stored in the smart card** (column 10, lines 60-67). (emphasis added)" This statement appears to contradict the earlier statement, and applicants respectfully request clarification on this matter.

The remarks below are based on the statement in the most recent Office Action.

In any event, applicants submit that for the reasons discussed below, even if Chaney discloses a key that is permanently stored in the smart card, amended claims 1-7 are patentably distinguishable over the cited prior art references.

The present invention employs the concept of **secret sharing** which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/video stream from a service provider (page 5, lines 4-7). In one embodiment, a first seed value received in a smart card, and a second seed value, permanently stored in the smart card are used to generate a symmetric key (page 5, line 31 - page 6, line 20). In that regard, claim 1 has been amended to recite:

> *(c) generating said scrambling key using said first seed value received in said smart card and a second seed value* ***in a predetermined***

> ***function, whereby secret sharing is implemented**, said second seed value being permanently stored in said smart card (emphasis added)*

Similarly Claim 5 recites:

> *calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value which is permanently stored in said smart card and means for descrambling, **whereby secret sharing is implemented**, within said smart card (emphasis added)*

Applicants submit that nowhere do Chaney or Santis teach or suggest such a combination of features. Additionally, Applicants submit that Chaney and Santis fail provide any teaching or suggestion combining the references in the manner suggested.

Chaney teaches a system that uses first and second smart cards to produce an image that includes multiple image portions, such as picture in picture (PIP) or picture outside picture (POP). In this regard, the system of Chaney uses the known system of using entitlement management messages (EMM) and entitlement control messages (ECM), which are transmitted with the digital video stream, to control access to the video programs.

The EMM indicates entitlement to a particular service, e.g. all programming on a particular channel, or to a particular program offered by a service, e.g., one movie on a particular channel (col. 2, lines 55-60). The ECM data is used to generate a descrambling key after entitlement to the program has been verified. The ECM provides initialization data for key generation routines that are executed by the processor (col. 2, lines 61-67; col. 4, lines 12-14; col. 7, lines 12-16).

The ECM may be transmitted in encrypted form, in which case, the smart card must first descramble the ECM to derive the initialization data that is used to generate the descrambling key. The key for descrambling the ECM may be stored on the smart card when the card is issued to the user (col. 10, lines 40-47).

In this case, it is clear that a first key received by the smart card, and a second key stored in the smart card, according to Chaney do not correspond to the first and second seed values recited in the present claims, and are not used to implement a secret sharing scheme. According to Chaney, the key stored in the card is used to descramble the ECM to generate initialization data, which

corresponds to the key received in the card, and the initialization data is then used in another algorithm to generate the final descrambling key. That is, the stored key is used to derive the received key, which is in turn used to derive the descrambling key with another algorithm. By contrast, the method according to the present invention uses both the stored key **and** the received key in a predetermined function, whereby secret sharing is implemented. Chaney says nothing about, and provides no teaching or suggestion, regarding secret sharing, and the key stored in the smart card is used for an entirely different purpose, and in a different manner, than that according to the present invention.

Santis, as discussed in applicants' previous response, teaches the primitive of function sharing, which is a functional analog of secret sharing, and its use in a cryptosystem. The basic idea of function sharing is to split a hard to compute function into shadow functions, wherein the function becomes easy to compute at a given point value when given any threshold of shadow function evaluations at that point (see abstract).

The examiner states that "Santis discloses function sharing which is the equivalent to key sharing." In that regard, Santis states that "A secret sharing scheme is a one-time operation, in the sense that the shadows (shares) are revealed when the secret is reconstructed. In function sharing, the shadow functions are never revealed to anyone and therefore the secret (i.e., the function's intractability) is maintained and the function is reusable many times." (page 522, Introduction, second paragraph)." As such, applicants submit that a secret sharing scheme is distinguishable from a scheme that uses the function sharing primitives taught by Santis.

Furthermore, Santis teaches that "the function sharing primitive has two phases: the shadow function generation phase (an initialization) where programs $\{P_1, \ldots P_l\}$ are generated by a key generator for the input function f^1_{se} represented by tuple (pu,se)(randomly chosen by the function generator G), and the function reconstruction phase where a threshold (at least) of partial results $P_i(\alpha)$ are **created from a public input α** and combined to construct $f^1_{se}(\alpha)$. (emphasis added)" Santis does not teach or suggest using a received key **and a key permanently stored in a card** to generate a descrambling key.

Applicants submit that present claims 1-7 are patentably distinguishable over the suggested combination of Chaney and Santis since such a combination fails to teach or suggest a notable feature of the claims. As noted above, Chaney teaches using a key stored in a smart card to derive an initialization data, and then using the initialization data to derive the descrambling key. Santis teaches using a function sharing scheme that includes a function reconstruction phase where a threshold (at least) of partial results $P_i(\alpha)$ are created from a **public input α** and combined to construct $f^{-1}_{se}(\alpha)$. These are entirely different methods of generating a descrambling key or a desired function, and neither method includes the feature of implementing a secret sharing scheme using in a predetermined function using a first seed value received in a smart card and a second seed value permanently stored in the smart card as taught by the present invention. As such, Applicants submit that the references fail to teach a notable feature of the claims, and that claims 1 and 5, and the claims that depend therefrom, are distinguishable over the teachings of the cited prior art references.

Furthermore, applicants submit that the suggested combination is improper because neither reference teaches or suggests any motivation for combining the references in the manner suggested. Neither reference teaches or suggests implementing a secret sharing scheme using in a predetermined function using a first seed value received in a smart card and a second seed value permanently stored in the smart card as taught by the present invention. As described above, Chaney and Santis describe entirely different methods for generating a descrambling key or desired function. Neither reference teaches or suggests how a combination that uses these methods might operate, or why it would be desirable to modify Chaney or Santis to do so. In fact, as mentioned above, Santis states that function sharing is distinguishable from secret sharing. In view of the above, applicants respectfully submit that the suggested combination of Chaney and Santis is improper and constitutes improper hindsight reasoning.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
A. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 9/24/04

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to [Mail Stop AF], Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

9/24/04
Date

Linda Tindall
Linda Tindall